UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/605,605	06/28/2000	Carl M. Ellison	042390.P7709	5805

7590 12/18/2003

William W Schaal
Blakely Sokoloff Taylor & Zafman LLP
7th Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025

EXAMINER	
DARROW, JUSTIN T	

ART UNIT	PAPER NUMBER
2132	3

DATE MAILED: 12/18/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/605,605	Applicant(s) ELLISON ET AL.	
	Examiner Justin T. Darrow	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13 and 15-20* is/are rejected.

7)☒ Claim(s) *14* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *28 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *2*.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

1. Claims 1-20 have been presented for examination.

Claim Objections

2. Claim 11 is objected to because of the following informality: delete "11" in line 1 and replace with --1--. Appropriate correction is required.

3. Claim 19 is objected to because of the following informality: delete "16" in line 1 and replace with --18--. Appropriate correction is required.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 16-20 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 16 recites the limitation "the pseudonym" in line 6. There is insufficient antecedent basis for this limitation in the claim. This rejection can be overcome by inserting after "the" in claim 16, line 6 --at least one--.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-13 and 15-20 are rejected under 35 U.S.C. 102(b) as being anticipated by S. Brands, "Restrictive Blinding of Secret-Key Certificates."

As per claim 1, Brands illustrates a method comprising: generating a public key, $a = w^v$ (see page 11, section 3.1, step 1 and figure 1); placing a in $t_1{}^v (h\, h_i)^{t2}$ a (see page 11, section 3.1, step 2 and figure 1); hashing this value for form a hash value c' (see page 11, section 3.1, step 2 and figure 1); transforming hash value c' into c (see page 11, section 3.1, step 2 and figure 1); performing an operation to form $r = (x\, y^{s0i})^c w$ and sending to R_i (see page 11, section 3.1, step 3 and figure 1); and performing an inverse transformation to recover a digital signature of the value c', r' (see page 11, section 3.1 and figure 1).

As per claim 2, Brands further depicts that a and v are a public private key pair (see page 11, section 3.1, step 1 and figure 1).

As per claim 3, Brands moreover shows that a is written in $t_1{}^v (h\, h_i)^{t2}$ a (see page 11, section 3.1, step 2 and figure 1).

As per claim 4, Brands then discusses transforming hash value c' into c in $c = c' + t_2 \bmod v$, where $t_2 \bmod v$ is a random number (see page 11, section 3.1, step 2 and figure 1).

As per claim 5, Brands also mentions $r^{v} (h\ h_i)^{-c} = a$, where c is based on t_2 mod v , a random number (see page 11, section 3.1, step 3).

As per claim 6, Brands further suggests that R_i stores the pseudo-random value, t_2 mod v, after sending it to S, for subsequent computation (see page 11, section 3.1, steps 2 and 3, and figure 1).

As per claim 7, Brands next discusses the inverse transformation to recover the digital signature using the inverse of t_2 mod $r' = r\ t_1\ (h\ h_i)^{c' + t2\ div\ v}\ s_{1i}^{c'}$ (see page 11, section 3.1 and figure 1).

As per claim 8, Brands additionally points out signing the hash value with the private key s_{0i} (see page 11, section 3.1 and figure 1).

As per claim 9, Brands then states that the result includes the public key, y^{s0i}, $r = (x\ y^{s0i})^{c}\ w$ (see page 11, section 3.1, step 3 and figure 1).

As per claim 10, Brands also specifies sending to R_i (see page 11, section 3.1, step 3 and figure 1).

As per claim 11, Brands further describes storing the certificate for secure management of cryptographic keys (see page 2, section 1, first full paragraph).

As per claim 12, Brands describes a device with processing that contains a triple consisting of a secret key, a corresponding public key, and a matching certificate for a party to perform a cryptographic action (see page 8, section 2, paragraphs 2 and 3).

As per claim 13, Brands further specifies that this matching certificate as a certified key pair (see page 8, section 2, paragraph 3).

As per claim 15, Brands then discusses transforming hash value c' into c in $c = c' + t_2 \bmod v$, where $t_2 \bmod v$ is a random number (see page 11, section 3.1, step 2 and figure 1).

As per claim 16, Brands discloses a platform comprising: a transceiver and a device in communication with the transceiver which contains a pair consisting of a public key and matching certificate as a certified public key, and to a triple consisting of a secret key, a corresponding public key, and a matching certificate as a certified key pair (see page 8, section 2, paragraphs 2 and 3) in which the certificate is a digital signature of a hash value of a digital certificate with a public key, $r = (x\, y^{s0i})^{c} w$ (see page 11, section 3.1 and figure 1).

As per claim 17, Brands further illustrates placing a in $t_1^{v} (h\, h_i)^{t2}$ a (see page 11, section 3.1, step 2 and figure 1); hashing this value for form a hash value c' (see page 11, section 3.1, step 2 and figure 1); and transforming hash value c' into c (see page 11, section 3.1, step 2 and figure 1).

As per claim 18, Brands additionally points out signing the hash value with the private key s_{0i} (see page 11, section 3.1 and figure 1).

As per claim 19, Brands also elaborates that the certificate, $r = (x\ y^{s0i})^{c}\ w$, includes the digital signature of the transformed certificate hash value, c (see page 11, section 3.1 and figure 1).

As per claim 20, Brands then embodies that the certificate of such a triple is uncorrelated to the view of the signer in the issuing protocol (see page 10, section 3, first paragraph).

Allowable Subject Matter

8. Claim 14 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

The following is a statement of reasons for the indication of allowable subject matter:

Claim 14 is drawn to a device. The closest prior art, S. Brands, "Restrictive Blinding of Secret-Key Certificates," teaches a similar device. However, he neither shows nor implies erasing a second key pair after a communication session with the remotely located device has concluded (see page 8, section 2, paragraph 3). This particular feature explicitly recited in claim 14 renders it to have allowable subject matter.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (703) 305-3872 and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (703) 305-1830.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.

December 12, 2003

JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100